

# BEST AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

4)

(11)Publication number : 10-211191

(43)Date of publication of application : 11.08.1998

(51)Int.Cl.

A61B 5/117  
G06T 7/00  
H04L 9/32  
H04N 5/76  
// G06T 1/00

(21)Application number : 09-019208

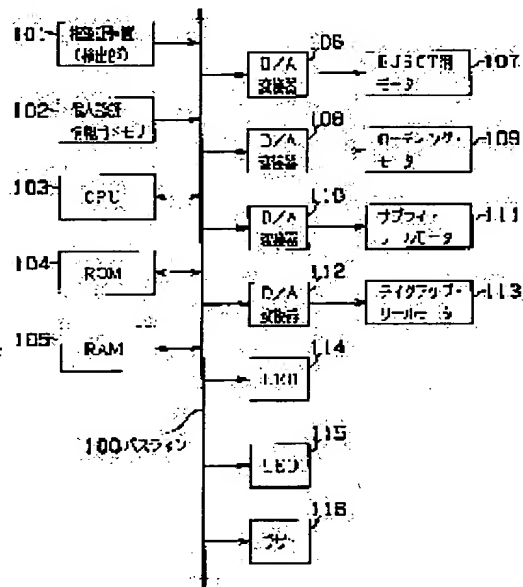
(71)Applicant : TOSHIBA CORP  
TOSHIBA AVE CORP

(22)Date of filing : 31.01.1997

(72)Inventor : YANAGIMOTO MASAO  
YONEDA MINORU  
OKUYAMA TAKEHIKO  
YAMADADERA SHINJI  
FUKUSHIMA MICHIIHIRO  
OSAWA SHINICHI**(54) RECORDING AND REPRODUCING DEVICE USING BIOLOGICAL INFORMATION AND ITS METHOD****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a recording and reproducing device using biological information and its method, which establishes absolute ownership with respect to the recording and reproducing device and a recording medium so as to protect copyright, privacy, etc.

**SOLUTION:** A finger authentication device 101 collates biological information detected by its detection part and that stored in a memory 102 for individual authentication information to execute the individual authentication operation of a person to be authenticated. At the time of passing individual authentication, a CPU 103 permits the operation of the recording and reproducing device to turn a motor 109 loading a cassette tape, a motor 107 ejecting a cassette and motors 111 and 113 driving a tape to be operable. On the other hand, at the time of not passing individual authentication, the CPU 103 does not permit the operation of the recording and reproducing device and stops the driving of all the motors.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-211191

(43) 公開日 平成10年(1998) 8月11日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

A 6 1 B 5/117  
G 0 6 T 7/00  
H 0 4 L 9/32  
H 0 4 N 5/76  
// G 0 6 T 1/00

A 6 1 B 5/10 3 2 2  
H 0 4 N 5/76 Z  
G 0 6 F 15/62 4 6 0  
H 0 4 L 9/00 6 7 3 D  
G 0 6 F 15/64 G

審査請求 未請求 請求項の数14 O L (全 21 頁)

(21) 出願番号 特願平9-19208

(22) 出願日 平成9年(1997) 1月31日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(71) 出願人 000221029

東芝エー・ピー・イー株式会社

東京都港区新橋3丁目3番9号

(72) 発明者 柳本 正雄

神奈川県横浜市磯子区新杉田町8番地 株  
式会社東芝マルチメディア技術研究所内

(72) 発明者 米田 稔

神奈川県横浜市磯子区新杉田町8番地 株  
式会社東芝マルチメディア技術研究所内

(74) 代理人 弁理士 伊藤 進

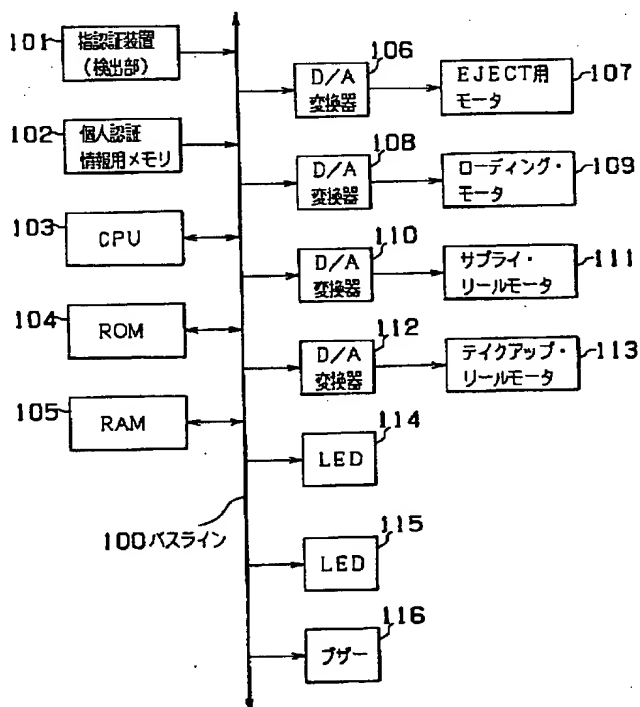
最終頁に続く

(54) 【発明の名称】 生体情報を使用する記録再生装置及び記録再生方法

(57) 【要約】

【課題】 記録再生装置および記録媒体に対して絶対的な所有権を確立し、著作権やプライバシー等を保護可能な、生体情報を使用する記録再生装置及び記録再生方法を提供すること。

【解決手段】 指認証装置101は、その検出部により検出された生体情報と個人認証情報用メモリ102に記憶されている生体情報との照合を行い、被認証者の個人認証動作を行う。個人認証をパスすると、CPU103は、記録再生装置の動作を許可し、カセットテープをローディングさせるモータ109やカセットをイジェクトさせるモータ107、テープ駆動を行うモータ111、113を動作可能な状態とする。一方、個人認証をパスしなかった場合、CPU103は、記録再生装置の動作を許可せず、一切のモータ駆動を停止する。



**【特許請求の範囲】**

【請求項1】 本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、

少なくとも1人分の生体情報を記憶する個人認証情報記憶手段と、

前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、

前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、

前記装置制限事項記憶手段に記憶された生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項管理手段と、

装置の動作状態を検出する装置動作検出手段と、

前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、

前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体とを具備したことを特徴とする生体情報を使用する記録再生装置。

【請求項2】 前記生体情報検出手段は、皮膚の接触により生じる電気特性の変化に対応して、一次元の電気信号分布を形成する表面形状センサにより構成されることを特徴とする請求項1に記載の生体情報を使用する記録再生装置。

【請求項3】 前記生体情報検出手段と前記装置動作検出手段とは、一体に形成されていることを特徴とする請求項1に記載の生体情報を使用する記録再生装置。

【請求項4】 前記個人認証情報記憶手段、並びに装置制限事項記憶手段は、前記記録再生媒体上の所定のエリアに設けられていることを特徴とする請求項1に記載の生体情報を使用する記録再生装置。

【請求項5】 前記生体情報検出手段は、皮膚の接触において、接触面の圧力を高める方向へ皮膚が移動することによって生体情報の検出が行われることを特徴とする請求項3に記載の生体情報を使用する記録再生装置。

【請求項6】 前記生体情報検出手段は、自動または手動で移動する手段を備え、個人認証のための生体情報を検出する際に自動または手動で装置外部に移動し、個人認証後に自動または手動で装置内部に移動することを特徴とする請求項1に記載の生体情報を使用する記録再生装置。

【請求項7】 本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、

前記生体情報を検出する方法により得られた生体情報と、少なくとも1人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、

前記生体情報記憶手段に記憶された生体情報に対応して設定された、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する方法と、

装置の動作状態を検出する方法と、

前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法とを具備したことを特徴とする生体情報を使用する記録再生方法。

【請求項8】 本体またはリモコンに設けられ、生体情報を検出する第1の生体情報検出手段と、

少なくとも1人分の生体情報を記憶する第1の個人認証情報記憶手段と、

前記第1の生体情報検出手段により得られた生体情報と、

前記第1の個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う第1の個人認証手段と、

前記第1の個人認証情報記憶手段に記憶される生体情報に対応して設定された装置の使用制限事項を記憶する第1の装置制限事項記憶手段と、

前記第1の装置制限事項記憶手段に記憶された生体情報の登録、並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録、変更、並びに削除を行う第1の装置制限事項管理手段と、

装置の動作状態を検出する第1の装置動作検出手段と、

前記第1の装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて、該装置の動作を制御する第1の装置動作制御手段と、

前記第1の装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録または再生動作が行われる第1の記録再生媒体とを備え、前記第1の個人認証情報記憶手段、並びに第1の装置制限事項記憶手段が、前記第1の記録再生媒体上の所定のエリアに設けられた第1の記録再生装置と、

本体またはリモコンに設けられ、生体情報を検出する第2の生体情報検出手段と、

少なくとも1人分の生体情報を記憶する第2の個人認証情報記憶手段と、

前記第2の生体情報検出手段により得られた生体情報

と、前記第2の個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う第2の個人認証手段と、

前記第2の個人認証情報記憶手段に記憶される生体情報に対応して設定された装置の使用制限事項を記憶する第2の装置制限事項記憶手段と、

前記第2の装置制限事項記憶手段に記憶された生体情報の登録、並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録、変更、並びに削除を行う第2の装置制限事項管理手段と、

装置の動作状態を検出する第2の装置動作検出手段と、前記第2の装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて、該装置の動作を制御する第2の装置動作制御手段と、

前記第2の装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録または再生動作が行われる第2の記録再生媒体とを備え、前記第2の個人認証情報記憶手段、並びに第2の装置制限事項記憶手段が、前記第2の記録再生媒体上の所定のエリアに設けられた第2の記録再生装置と、

少なくとも前記第1または第2の記録再生装置の何れか一方に設けられた、前記第1および第2の記録媒体に記憶されている個人認証情報データを比較する個人認証情報データ比較手段と、

前記個人認証情報データ比較手段により比較した結果が一致した場合のみ、前記第1の記録再生装置からの再生情報が、前記第2の記録再生装置にてダビング記録可能とする手段とを具備したことを特徴とする生体情報を使用する記録再生装置。

【請求項9】 本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する第1の方法と、

前記生体情報を検出する第1の方法により得られた生体情報と、少なくとも1人分の個人認証情報である生体情報を記憶する第1の生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う第1の方法と、

前記第1の生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する第1の装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する第1の方法と、

装置の動作状態を検出する第1の方法と、

前記装置の動作状態を検出する第1の方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の第1の記録再

生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する第1の方法とを備え、前記第1の個人認証情報記憶手段、並びに第1の装置制限事項記憶手段が、前記第1の記録再生媒体上の所定のエリアに設けられた第1の記録再生装置と、

本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する第2の方法と、

前記生体情報を検出する第2の方法により得られた生体情報と、少なくとも1人分の個人認証情報である生体情報を記憶する第2の生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う第2の方法と、

前記第2の生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する第2の装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する第2の方法と、

装置の動作状態を検出する第2の方法と、

前記装置の動作状態を検出する第2の方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の第2の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する第2の方法とを備え、前記第2の個人認証情報記憶手段、並びに第2の装置制限事項記憶手段が、前記第2の記録再生媒体上の所定のエリアに設けられた第2の記録再生装置と、

少なくとも前記第1または第2の記録再生装置の何れか一方に設けられた、前記第1および第2の記録媒体に記憶されている個人認証情報データを比較する方法と、前記個人認証情報データを比較する方法により比較した結果が一致した場合のみ、前記第1の記録再生装置からの再生情報が、前記第2の記録再生装置にてダビング記録可能とする方法とを具備したことを特徴とする生体情報を使用する記録再生方法。

【請求項10】 本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、

少なくとも1人分の生体情報を記憶する個人認証情報記憶手段と、

前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、

前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、

前記装置制限事項記憶手段に記憶された生体情報の登

録、並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項管理手段と、

装置の動作状態を検出する装置動作検出手段と、  
前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、

前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体と前記個人認証情報記憶手段、並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、

暗号化またはスクランブルされた記録データを作成する手段と、

暗号化またはスクランブルされたデータを記録する際に、暗号化またはスクランブルを解くためのキーデータを、前記所定の個人認証情報を用いて作成する手段と、  
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを前記記録再生媒体に記録する手段とを具備したことを特徴とする生体情報を使用する記録再生装置。

【請求項 11】 本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、

少なくとも 1 人分の生体情報を記憶する個人認証情報記憶手段と、

前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、

前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、

前記装置制限事項記憶手段に記憶された生体情報の登録、並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項管理手段と、

装置の動作状態を検出する装置動作検出手段と、  
前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、

前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体と前記個人認証情報記憶手段、並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、

暗号化またはスクランブルされた記録データを作成する手段と、

暗号化またはスクランブルされたデータを記録する際に、暗号化またはスクランブルを解くためのキーデータを、

前記所定の個人認証情報を用いて作成する手段と、  
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを前記記録再生媒体に記録する手段と、

再生時に個人認証データを入力し、登録してある個人認証データと比較する比較手段と、

前記比較手段による比較結果が、一致していた場合のみ、前記記録媒体からキーデータを読み出し、読み出したキーデータに基づいて暗号を解く、またはデスクランブルする手段とを具備したことを特徴とする生体情報を使用する記録再生装置。

【請求項 12】 本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、

前記生体情報を検出する方法により得られた生体情報と、少なくとも 1 人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、

前記生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する方法と、

装置の動作状態を検出する方法と、  
前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法と前記個人認証情報記憶手段、並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、

暗号化またはスクランブルされた記録データを作成する方法と、

暗号化またはスクランブルされた前記記録データを記録する際に、暗号化またはスクランブルを解くキーデータを、前記所定の個人認証データを用いて作成する方法と、

前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを記録媒体に記録する方法とを具備したことを特徴とする生体情報を使用する記録再生方法。

【請求項 13】 本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、

前記生体情報を検出する方法により得られた生体情報と、少なくとも 1 人分の個人認証情報である生体情報を

記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、

前記生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する方法と、

装置の動作状態を検出する方法と、

前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法と前記個人認証情報記憶手段、並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、暗号化またはスクランブルされた記録データを作成する方法と、

暗号化またはスクランブルされた前記記録データを記録する際に、暗号化またはスクランブルを解くキーデータを、前記所定の個人認証データを用いて作成する方法と、

前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを記録媒体に記録する方法と、

再生時に個人認証データを入力し、登録してある個人認証データと比較する方法と、

比較結果が一致していた場合にのみ、前記記録媒体からキーデータを読み出して、読み出したキーデータにもとづいて暗号を解く、またはデスクランブルする方法とを具備したことを特徴とする生体情報を使用する記録再生方法。

【請求項 14】前記リモコンは、

生体情報を検出する手段と、

被制御装置を選択する手段と、

被制御装置の機能を選択する手段と、

前記生体情報と被制御装置を選択する情報と被制御装置の機能を選択する情報を、被制御装置を制御する信号に変換する手段と、

前記被制御装置を制御する信号を出力する手段とを具備したことを特徴とする請求項 1 から 6 乃至 8, 10, 11 に記載の生体情報を使用する記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、映像、音声、またはデジタルデータ等を記録・再生する記録再生装置に係り、特に生体情報検出手段を有し、検出された生体情報に基づいて制御を為す、生体情報を使用する記録再生装置及び記録再生方法に関する。

【0002】

【従来の技術】近年、情報化社会の高度化に伴い、個人または企業が取り扱う情報量、特に電子化された情報データ量は増加の一途をたどっている。これら情報データの多くは対外的に秘密保持を要するものが普通である。特に、情報の商品化が急速に進んだ現代においては、個人のプライバシーや企業秘密等の保護に加え、著作権等の保護などの様々な観点から、これら情報の扱いは非常に重要なものとなってきている。そのため、これら様々な情報、特にデジタル化された情報の漏洩や改ざん、或いは不正コピー等に対する防御方法（セキュリティシステム）が問われるようになってきている。

【0003】ホストコンピュータやワークステーション等のネットワークや、早くから電算化されている金融関係のシステムでは、記録されている個人に関する情報やシステムの操作権（アクセス権）は厳重に守られており、暗証番号やパスワードといったキーワードや、光カードや IC カードを使用した物理的な施錠等が用いられている。

【0004】このように、ネットワークを介してのプライバシーや著作権侵害等に関する保護対策は、かなりの水準にまで達しており、相当の成果をあげている。

【0005】これに対し、ネットワークを介さないローカルなシステム、例えば、映像や音声情報等を扱う記録再生装置を基本とするシステムでは、著作権を無視した不正なコピー等が自由に行われ、国際的に問題化している。

【0006】以下、図 17 を参照しながら記録媒体としてテープ媒体を用いた従来の記録再生装置（ビデオテープレコーダ）について説明を行う。図 17 は従来の記録再生装置の構成を示すブロック図である。

【0007】図 17 において、ビデオテープレコーダ（以下、VTR）などの記録再生装置は、バスライン 100 に接続された CPU 103 がバスライン 100 を介し、制御信号を各種モータ（107, 109, 111, 113）に対して供給することによりメカ動作が行われる。CPU 103 の制御プログラムは ROM 104 に格納されている。各モータは、対応する各 D/A 変換器（106, 108, 110, 112）にモータ動作に対応した制御信号が供給されることによりそれぞれ動作する。EJECT 用モータ 107 は、挿入されている（ローディング状態にある）カセット（ビデオカセットテープ）を排出する動作を行うものである。ローディング・モータ 109 は、カセット挿入後、移動式テープガイドによりテープを所定の位置まで引き出し、図示しない回転ドラムヘッドにテープを巻き付けたり、カセットを排出する際、前記回転ドラムヘッドに巻き付いているテープをカセット内に巻き戻す動作を行うものである。サプライ・モータ 111 およびテイクアップ・リールモータ 113 は、それぞれ図示しないサプライリールおよびテ

イクアップリールを回転させてテープの巻き取りおよび送り出しを制御してテープ駆動動作を行うものである。

【0008】以上の構成において、カセットをVTRに挿入すると、ローディング・モータ109が動作して、自動的にテープが回転ドラムヘッドに巻き付けられる（テープローディングが為される）。この状態で、操作者がVTRの再生ボタンを押下すると、サプライ・リールモータ111およびテイクアップ・リールモータ113が動作して、テープ駆動動作が行われ、テープの再生を行うことができる。また、操作者がVTRの記録ボタンを押下すると、記録保護がなされていないカセットの場合、再生時と同様にサプライ・リールモータ111およびテイクアップ・リールモータ113が動作して、テープ駆動が行われ、テープに記録することができる。

【0009】以上のように、従来の記録再生装置（VTR）では、誰がVTRを操作しようと、テープへの記録またはテープ再生を自由に行うことが可能である。尚、所有者情報（文字）をテープ中に画像情報として挿入・記録したり、テープ中の所定の領域にコンテンツ情報を挿入したり、或いは6mmデジタルカセットの場合には、カセットに設けられたMIC（Memory In Cassette）と呼ばれるICメモリ上に所有者およびコンテンツ情報を記録しておくことで、再生時、表示画面上にそれらの情報を表示させることにより、VTR内に挿入されたカセットの所有者およびコンテンツ情報を操作者等に知らしめることは可能ではあるが、当該テープ（カセット）への記録またはテープ再生を自由に行うことは可能であり、物理的に操作不能状態とはならない。

【0010】このように、上記従来の記録再生装置では、何れも所有者や著作権者の情報やコンテンツ情報を画面上に表示させるのみであり、記録媒体上に記録されている情報やシステムの操作権（アクセス権）の保護による、所有者や著作権者の権利保護は、一切為されない。即ち、上記従来の記録再生装置では、いわゆる著作物を自由にコピー（ダビング）し、複製を作成可能である。

【0011】近年、技術の進歩に伴い、映像や音声情報等をほとんど劣化させることなく複製を容易に作成することが可能となっており、特に、デジタル映像やデジタル音声情報等の場合、完全に同一な複製が作成可能であるため、早急な対策が求められている。

【0012】さらに、上記従来の記録再生装置は、既述のコンピュータシステムと異なり、暗証番号やパスワードといったキーワードや、光カードやICカードを使用した物理的な施錠機能を持たないため、第三者によるシステム（装置）の無断使用を防止する手段が無く、第三者により記録媒体への誤記録や誤消去が為される可能性を有すると共に、前記記録再生装置（ムービー等のポータブル機器）の盗難時等において、パーソナル映像や極秘映像（ビデオ撮影による記録映像等）のセキュリティ

一確保の手段が皆無である。

【0013】

【発明が解決しようとする課題】上記の如く、従来の記録再生装置では、セキュリティ確保の手段を有しないため、所有者以外の人間が無断で装置を操作したり、他人のテープを自由に再生することが可能であり、個人（所有者）のプライバシーが保護されないという問題があった。さらには、無断で装置を操作する所有者以外の人間が、装置の操作を誤って、テープの誤記録や誤消去が為される可能性を有するなどの問題があった。

【0014】そこで、本発明はこのような問題に鑑み、テープやディスクなどを記録媒体とする記録再生装置および記録媒体に対して絶対的な所有権を確立し、著作権やプライバシー等を保護すると共に、記録媒体への第三者による誤記録、誤消去を防止することが可能な、生体情報を使用する記録再生装置及び記録再生方法を提供することを目的とするものである。

【0015】

【課題を解決するための手段】上記の目的を達成するために、本発明の記録再生装置は、本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、少なくとも1人分の生体情報を記憶する個人認証情報記憶手段と、前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、前記装置制限事項記憶手段に記憶された生体情報の登録、並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項管理手段と、装置の動作状態を検出する装置動作検出手段と、前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行いその認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、前記装置動作制御手段の制御により映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体とを具備したことを特徴とするものである。

【0016】また、本発明の記録再生方法は、本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、前記生体情報を検出する方法により得られた生体情報と、少なくとも1人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、前記生体情報記憶手段に記憶された生体情報に対応して設定された装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録、並びに削除、および生体情報に



対応して設定された、装置の使用制限事項の登録、変更、並びに削除を行う装置制限事項を管理する方法と、装置の動作状態を検出する方法と、前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法とを具備したことを特徴とするものである。

【0017】ここで、上記記載の発明によれば、記録再生装置を使用する際に個人認証が行われ、認証されたもののみが記録再生装置の使用を許される。また、認証には記録再生装置内に登録された個人認証情報が用いられ、認証情報として生体情報（指情報等）が用いられる。これにより、記録再生装置が盗難にあった場合など、正常に動作しない（第三者による操作不可能）ため盗難防止効果が得られる。また、個人使用（パーソナルユース）のための装置の場合、第三者による記録が出来ないため誤記録、誤消去を防ぐことができると共に、テープなどの媒体に記録されているパーソナル情報を保護することができる。

【0018】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は本発明の実施の形態に係る生体情報による個人認証装置を具備した記録再生装置を示すブロック図である。

【0019】本発明の実施の形態では、生体情報による個人認証装置として指認証装置を具備したビデオカセットテープを利用したムービーなどの記録再生装置を例に説明を行う。

【0020】図1において、ビデオテープレコーダ（以下、VTR）等の記録再生装置は、バスライン100に接続されたCPU103がバスライン100を介し、各種モータ（107、109、111、113）に対し、制御信号を供給することにより、メカの動作が行われるものである。CPU103の制御プログラムはROM104に格納されている。各モータは、対応する各D/A変換器（106、108、110、112）に対し、モータ動作に対応した所定の制御信号が供給されることによりそれぞれ動作するものである。

【0021】そして、EJECT用モータ107は、挿入されている（ローディング状態にある）カセット（ビデオカセットテープ）を排出する動作を行うものである。ローディング・モータ109は、カセット挿入後、移動式テープガイドによりテープを所定の位置まで引き出し、図示しない回転ドラムヘッドにテープを巻き付けたり、カセットを排出する際、前記回転ドラムヘッドに巻き付いているテープをカセット内に巻き戻す動作を行うものである。サプライ・モータ111およびテイクア

ップ・リールモータ113は、それぞれ図示しないサブライリールおよびテイクアップリールを回転させてテープの巻き取りおよび送り出しを制御してテープ駆動動作を行うものである。

【0022】また、指認証装置（検出部）101は、例えば指を乗せることにより、あらかじめ個人認証情報用メモリ102に記憶されている情報に基づいて個人認証動作を行うものである。個人認証情報用メモリ102は、後述する登録モードにより個人認証情報の登録、変更並びに削除等が行われる。尚、CPU103は、前記装置のメカ動作（各モータ）の制御を行うと共に、個人認証のための演算処理動作を行う。そのための制御プログラムが前記ROM104に格納されている。

【0023】さらに、前記バスライン100には、前記指認証装置（検出部）101やCPU103の動作状態をモニターするためのLED114、115やブザー116が接続されている。

【0024】次に、本発明の生体情報による個人認証装置を具備した記録再生装置の個人認証動作について、図2を参照しながら説明を行う。図2は個人認証動作手順を示したフローチャートである。

【0025】上記の構成において、操作者（被認証者）により装置の電源が投入、またはカセットテープがVTRに挿入されると、VTR（本発明の生体情報による個人認証装置を具備した記録再生装置）は、個人認証動作を開始する（ステップS1、S2）。即ち、指認証装置101は、その検出部により検出された生体情報（指情報）と、個人認証情報用メモリ102に記憶されている生体情報（指情報）との照合を行い、被認証者がVTR（記録再生装置）に登録されている人物か否かの個人認証動作を行う。当然に、個人認証動作をパスしないと機器を動作させることはできない。個人認証動作のための手順（プログラム）はROM104に格納されていて、フラッシュメモリやICメモリ等の書き換え可能な個人認証情報用メモリ102に保存されている個人認証情報（指情報）をもとに、前記プログラムにしたがって、CPU103により個人認証が行われる。

【0026】指照合の結果、登録者であることが判明した場合、即ち指認証装置101の検出部により検出された生体情報（指情報）と、個人認証情報用メモリ102に記憶されている生体情報（指情報）とが一致し、被認証者が認証された場合、CPU103は、VTR（記録再生装置）の動作を許可し、これにより、メカ部、即ち、カセットテープをローディングさせるモータ109やカセットをイジェクトさせるモータ107、テープ駆動を行うモータ111、113を動作可能な状態となり（ステップS3、S4）、記録・再生などの通常動作を行うことが可能となる（ステップS5）。

【0027】一方、前記指照合の結果、登録者でないと判別された場合、即ち指認証装置101の検出部により

検出された生体情報（指情報）と、個人認証情報用メモリ102に記憶されている生体情報（指情報）とが一致せず、被認証者が認証なかった場合、CPU103は、VTR（記録再生装置）の動作を許可せず、一切のモータ駆動を停止する（ステップS3、S6）。さらに、認証されなかった前記被認証者の指情報を個人認証情報用メモリ102に保存する（ステップS7）。これにより、正規登録者（VTR装置の所有者等）は、不正にVTR（記録再生装置）を操作しようとした者を特定するための情報を得ることができる。

【0028】本実施の形態では、記録媒体としてビデオカセットテープを使用するムービーを例に説明したが、これに限定されるものではなく、例えば、記録媒体がディスク状の物でも良いし、ICメモリ状のものでも良い。また、モータ制御用と個人認証演算用のCPU、ROM、並びにRAMを、前記CPU103、ROM104、並びにRAM105の1セットで兼ねて（共用して）いるが、それぞれ別々の構成としても良い。さらに、個人認証のための生体情報として指情報を用いているが手や足、目など他の生体情報でも勿論良い。

【0029】以上のように、生体情報によって個人認証を行い、認証されない場合、記録再生装置の動作を停止させる機能を設けたので、記録再生装置が盗難にあった場合でも、登録者（所有者等）以外によって、前記記録再生装置を正常に動作させることは不可能であり、これにより、前記記録再生装置の盗難を防止する効果を得られる。また、記録再生装置が個人専用の装置（パーソナルユース）として使用される場合、第三者による操作が不可であるため、誤記録、誤消去を防ぐことが出来ると共にテープ等の記録媒体に記録されているパーソナル情報を保護することができる。

【0030】次に、本発明の記録再生装置の個人認証情報用メモリ102への認証情報（指情報）の登録および取り消し方法の一例について説明を行う。尚、本発明の記録再生装置には、スーパーユーザー登録モード／取り消しモード、および一般ユーザー登録モード／取り消しモードを有するものとして説明を行う。

【0031】先ず、記録再生装置（以下、単に装置ともいう）の絶対使用者であるスーパーユーザーに関する登録モードについてであるが、原則、スーパーユーザーの登録は、例えば、装置の新規購入時などのスーパーユーザー未登録時においてただ1人のみ行うことができる。スーパーユーザーの登録を行おうとする者は、記録再生装置に設けられた図示しない操作手段によって、スーパーユーザー登録モードを選択し、指認証装置101の検出部に指を乗せる。すると、前記CPU103は、指認証装置101により検出された個人認証情報（指情報）を、スーパーユーザーの個人認証情報（指情報）として個人認証情報用メモリ102に記憶し、これによりスーパーユーザーの登録が為される。

【0032】次に、一般ユーザー登録モードについてであるが、一般ユーザーの登録は、スーパーユーザーにより認められた、記録再生装置の操作許可者（家族や友人など）についてのみ登録を行うことができる。このため、一般ユーザーの登録は、既述の個人認証動作に基づいて、指認証装置101によりスーパーユーザーが認証された後にのみ行うことができる。

【0033】指認証装置101によりスーパーユーザーが認証され、記録再生装置が操作可能状態となった後、図示しない前記操作手段によって、一般ユーザー登録モードを選択し、指認証装置101の検出部に登録する一般ユーザーの指を乗せる。これにより、指認証装置101により検出された個人認証情報（指情報）は、一般ユーザーの個人認証情報（指情報）として個人認証情報用メモリ102に記憶され、一般ユーザーの登録が為される。尚、一般ユーザー登録モードになっている間は何人でも登録することができ、モードを解除すると登録モードは終了し、一般ユーザーの登録が終了する。また、上記登録において、指を一本だけ登録した場合、登録した指をケガした場合など、個人認証の際に、認識（認証）されないという可能性があるため、他の指を複数本同時に登録しておくとも良い。

【0034】次に、スーパーユーザーの登録取り消しモードについてであるが、スーパーユーザーの登録取り消しは、当然スーパーユーザーのみにより可能である。スーパーユーザー登録の取り消しは、スーパーユーザーが認証された後、前記記録再生装置に設けられた図示しない操作手段によりスーパーユーザー登録取り消しモードを選択し、スーパーユーザーが指認証装置（検出部）101に指を乗せる。これにより、指認証装置101により検出された個人認証情報（指情報）、即ち、被認証者と一致する個人認証情報（スーパーユーザーの指情報）が個人認証情報用メモリ102から消去され、これにより、スーパーユーザーの登録が取り消される。この際、一般ユーザー登録が為されていても、スーパーユーザーの登録が取り消されるのと同時に全て取り消される。

【0035】次に、一般ユーザーの登録取り消しモードについてであるが、一般ユーザー登録の取り消しは、登録時と同様にスーパーユーザーが認証された後、前記図示しない操作手段により一般ユーザー登録取り消しモードを選択し、一般ユーザーが指認証装置（検出部）101に指を乗せる。これにより、指認証装置101により検出された個人認証情報（指情報）、即ち、被認証者と一致する個人認証情報（一般ユーザーの指情報）が個人認証情報用メモリ102から消去され、これにより、一般ユーザーの登録が取り消される。

【0036】ところで、上記記録再生装置には、前記図1に示す如くに、LED114、115やブザー116などが設けられており、例えば上記被認証者を認証中（指認証装置（検出部）101に指が乗っている間）、

LED114を点灯させたりブザー116から音を発し、認証された場合、LED115を点灯させたり認証中とは異なる音色をブザー116から発することにより被認証者に装置が動作中（認証中）であることを知らせるようにしてもよい。これにより、認証状況を被認証者に容易に知らせることができる。尚、本実施の形態では、被認証者に装置が動作中（認証中）であることを知らせる方法の一例として、LEDとブザーを使用しているが、記録再生装置がムービー（ハンディカメラ一体型記録再生装置）などの場合には、ファインダー内のモニタ部に認証状況をマークやアイコン、或いは文字等を用いて表示するようにしても良いし、外部モニタに接続されている装置の場合は、認証状況を外部モニタに表示するようにしても良い。

【0037】以上、個人認証情報および各個人認証情報毎に設定される装置に対する設定条件の対応付け（各個人毎の装置の使用制限）等を、記録再生装置の個人認証情報用メモリ102に登録し、これに基づいて、各個人に対する装置の使用制限を各記録再生装置毎で行う場合について説明したが、各個人に対する装置の使用制限を、各記録媒体毎に行うことも可能である。

【0038】次に、個人認証情報および各個人認証情報毎に設定される装置に対する設定条件の対応付け（各個人毎の装置の使用制限）を、各記録媒体毎に行う場合について説明する。

【0039】ここでは、民生用のデジタルVTRを例に説明する。記録媒体への登録は、当該記録媒体に対して記録または再生を最初に行う者に対して最初の権利付与が行われる。例えば、未記録のカセットテープに記録を開始する際、個人認証が行われ、認証された個人認証情報および記録媒体に対する設定条件の対応付け（権利付与）が登録される。この後、他のユーザーの登録を行っても良い。尚、権利付与に関する登録内容としては、登録ユーザーの当該記録媒体の特定箇所への記録の許可／禁止、および再生の許可／禁止などである。

【0040】また、再生専用のカセットテープ（記録媒体）の再生を最初に行う者に対しても同様の権利付与が行われる。即ち、当該記録媒体を初めて再生する際、個人認証が行われ、認証された個人認証情報および記録媒体に対する設定条件の対応付け（権利付与）が登録される。この後、同様に、他のユーザーの登録を行っても良い。権利付与に関する登録内容としては、登録ユーザーの当該記録媒体の特定箇所の再生の許可／禁止などである。

【0041】前記権利付与に関する登録内容（カセットテープ毎の情報）は、カセットテープに埋め込まれたRAM（MIC）に記録される。

【0042】このようにして登録が行われたカセットテープが民生用のデジタルVTRに挿入されると、VTR（本発明の生体情報による個人認証装置を具備した記

録再生装置）は、図1の指認証装置101の検出部により検出された生体情報（指情報）と、カセットテープに埋め込まれたRAM（MIC）に記憶されている生体情報（指情報）との照合が行われ、被認証者が登録ユーザーか否かの個人認証が行われる。登録ユーザーであることが確認されると、確認（認識）されたユーザーの権利付与に関する登録内容が参照され、その登録内容にそった操作のみが許可され、実施可能となる。尚、前記被認証者が登録ユーザーか否かの個人認証（第2の認証）は、既述の記録再生装置自体に関する認証（第1の認証）をパスして、記録再生装置（民生用のデジタルVTR）の動作が可能な状態、即ち、記録・再生などの通常動作を行うことが可能な状態にて行われる。また、前記第1の認証と第2の認証は同時に行われても良いし、別々に行われても良い。

【0043】前記カセットテープに埋め込まれたRAM（MIC）に記録された前記権利付与に関する登録内容（カセットテープ毎の情報）の登録の変更および削除は、それぞれの設定の権利を持つ者が行うことができる。即ち、記録および再生の権利を有する者は記録および再生の何れの権利についても削除可能であり、再生のみの権利を有する者は再生の権利についてのみ削除可能である。尚、記録の権利を有する者も再生の権利を有する者もない状態は、誰もが権利者になれる状態であり、未記録状態と同じ状態である。

【0044】図3はメモリインカセットのメモリのデータストラクチャ例である。図3において、DVC（民生用デジタルVTR）の規格で決められたメインエリア201は、APM, BCID, CASSETTE ID, TAPE LENGTH, TITLE ENDの各エリアにより構成される。

【0045】また、オプションエリア202には、通常、タイトルなどテキストデータが記録される。本実施の形態では、指照合個人認証データと各個人毎の装置に対する設定条件がこのオプションエリアに記録される。MIC（メモリインカセット）に記録されるシステムデータは、規格で、パック単位のデータストラクチャとなっており、1パックはヘッダー1バイトとデータ5バイトからなる。

【0046】指照合個人認証データは精度によりデータ量が異なる。同様に、各個人毎の装置に対する設定条件もユーザーにより条件の数が異なる。このため、オプションエリア202には、同図に示すように、指照合個人認証データ（finger datalength）、個人毎の装置に対する設定条件データの全データ量（function datalength）それぞれについて、データ長を予め記録しておく。

【0047】このような構成（フォーマット）とすることにより、メモリインカセットのメモリのデータストラクチャは、複数のシステムデータパックで構成されるこ

とになり、規格のTEXTデータの構造と同じになる。

【0048】以上のようにカセットテープを管理することで、誤って他人の重要な情報を消去してしまったり、自己の重要な情報を他人に消去されることを未然に防止することができる。また、他人に見られたくないデータを自己以外の者に対しては再生不可とすることができ、プライバシーの保護が可能となる。さらに、カセットテープが盗難にあってもデータを再生される心配がない。

【0049】ところで、上述の実施の形態では、個人認証情報または各個人毎の装置に対する設定条件を登録しておく箇所は、メモリ付きカセットのメモリであるとして説明を行ったが、これに限定する必要はない。

【0050】即ち、テープ内の所定位置、例えば、サブコートやVAUXのシステムデータ記録エリアに、記録プログラム毎に登録データを記録することも可能である。この場合、図3で示した個人認証情報、または各個人毎の装置に対する設定条件のシステムデータパックをそのまま、サブコードやVAUXのオプションエリアに記録すればよい。

【0051】また、個人認証情報または各個人毎の装置に対する設定条件を登録しておく箇所として、カセットに貼るラベルにバーコードで記録して、デッキ本体或いは専用装置がバーコードリードするようなシステムでもよい。

【0052】さらには、インターフェースを本体或いはリモコンに有する記録再生装置として、ビデオテープレコーダ以外の、例えば、DVD-RAM（書き込み可能デジタルビデオディスク）レコーダであってもよい。この場合、指照合個人認証データと各個人毎の装置に対する設定条件データを記録する箇所は、DISCのユーザーデータを記録する箇所であるTOC（table of contents）部分とする。この場合、図7で示した指照合個人認証データおよび各個人毎の装置に対する設定条件データは、DISCのTOCデータストラクチャに合わせて記録すればよい。

【0053】次に、生体情報（指情報）を検出する、前記図1に示した指認証装置101について簡単に説明を行う。図4は本発明で個人認証を行うための生体情報検出手段として使用される指認証装置の一例を示すブロック図である。

【0054】図4における指認証装置は、大きく分けて、指紋を入力するための指紋入力部10（生体情報検出電極）と、この指紋入力部10の出力に基づいて射影抽出（指紋情報）を求める射影計算部20と、この射影計算部20の出力に基づいてフィルタリング処理や照合計算を行なう信号処理部30と、この信号処理部30の出力に基づいてシステム制御、特徴登録、並びに1/F制御を行なう制御部40とで構成されている。この場合、射影計算部20～制御部40までが個体認証部となる。

【0055】図5は指紋入力部10を構成する表面形状センサの具体的な構成を示す図である。図5において、基板3の表面には複数の線状接触子電極2（生体情報検出電極）が一次元のアレイ状に設けられている。また、各線状接触子電極2は電極取り出しパッド5に繋がっている。

【0056】基板3の材料としては、例えば、ガラエポ等のプリント基板材料、セラミック板、あるいは絶縁被覆した金炉薄板などが用いられ、線状接触子電極2の材料としては、例えば、Cu薄膜、Au薄膜、Niメッキ薄膜、Pt薄膜、あるいはPd薄膜等、人体或いは動物の皮膚から出る汗等の体液に侵されない導電性材料がもちいられる。

【0057】また、線状接触子電極2の間隔は1/10mm程度で構成され、線状接触子電極2の数、すなわち、電極アレイの長手方向の長さは、通常、指の先端から第2関節を完全に含む程度の長さとなっている。

【0058】このように構成された表面形状センサを有する指紋入力部10によれば、線状接触子電極2に、指紋検出するべき指1が電極配列方向に対して直角方向に押し付けられると、隣接する線状接触子電極2で接触する指紋の凸部の量に応じて線状接触子電極2間の抵抗値が変化するので、一次元の抵抗分布が生じる。隣合う線状接触子電極2の間の指表面の抵抗値は、各電極取り出しパッド5から指1の長手方向に順次に読み取られる。

【0059】図6は、指表面の抵抗値の測定原理を説明するための指紋入力部10の等価回路である。

【0060】図6において、 $i+1$ 個の線状接触子電極 $2n$ （ $1 \leq n \leq i+1$ ）に対して指を押し付けたとき、隣接する線状接触子電極 $2n$ 、 $2n+1$ で接触する指紋の凸部の量に応じて線状接触子電極2間の抵抗値 $R_n$ が変化する。隣接する二つの線状接触子電極 $2n$ 、 $2n+1$ の間に、図示の如く、基準抵抗 $R_{ref}$ と定電圧源 $V_o$ とをアナログスイッチを介して接続する。このときの基準抵抗 $R_{ref}$ の両端の電位差 $V_n$ は次式で与えられる。

【0061】

$$V_n = R_{ref} \cdot V_o / (R_{ref} + R_n)$$

アナログスイッチを切り替えて、この電位差 $V_n$ を指の長手方向に順次に読み取り、この電位差 $V_n$ から算出された抵抗値 $R_n$ を時系列にプロットすることにより、図7に示すように、指の長手方向への多値射影信号と等価な抵抗値で表現された指紋情報を得ることができる。

【0062】なお、図7の横軸は隣接する線状接触子電極 $2n$ 、 $2n+1$ の位置を示しており、縦軸は抵抗値 $R_n$ を示している。また、多チャンネルとなるので、アナログスイッチとしてアナログマルチプレクサICを用いることにより、回路を小型化することができる。

【0063】次に、以上のように構成された指認証装置

101の生体情報検出電極（線状接触子電極）2の記録再生装置への取付位置について説明を行う。図8および図9は生体情報検出電極2が一体に形成された本発明に係る記録再生装置のスイッチキー（操作ボタン）を示した図である。

【0064】図8において、図8(a)はスイッチが押されていない状態を、図8(b)は指がスイッチを押している状態をそれぞれ示している。生体情報検出電極301はスイッチキー302の上面に配置され、支点303はスイッチキー302の手前（左側）に配置されている。

【0065】以上の構成において、スイッチ304を操作（押下）するために、キー302を指305で押すと、キー302の前方部分が押し下げられスイッチ304が押下されると共に、指305の腹部全体に力がかかることにより、指305の腹部が生体情報検出電極301に圧着されることになる。これにより、指認証装置101は、確実に生体情報を読み取ることができ、個人認証動作を行うことができる。

【0066】同様に、図9は、指305がスイッチキー402を引いている状態を示している。スイッチキー402には、垂直もしくは斜めに傾けて生体情報検出電極301が設けられている。

【0067】以上の構成において、スイッチ403を操作（押下）するために、指305の腹部にて、スイッチキー402を手前に引く（矢印方向にスライドさせる）ことにより、スイッチ403が押下される。このとき、指305の腹部全体に力がかかり、指305の腹部が生体情報検出電極301に圧着される。これにより、指認証装置101は、確実に生体情報を読み取ることができ、個人認証動作を行うことができる。

【0068】以上のようなスイッチ、即ち、スイッチ操作を行う際に必ず指305の腹部が生体情報検出電極301に圧着されるように構成されたスイッチを用いることにより、ユーザーは、個人認証が行われていることを意識することなく（気にすることなく）、記録再生装置の操作を行うことができる。

【0069】以上、ユーザーに対して、個人認証が行われていることをできるだけ意識させないようにユーザー（装置使用者）の生体情報を取得する方法（スイッチの構成）について説明したが（ムービー等の小型の装置に有効）、次に、本発明に係る記録再生装置に対して所定の操作を行おうとした際に、装置により個人認証の必要が明示的に示され、この要求に従ってユーザー（装置使用者）が個人認証を意識的に受ける場合、即ち、ユーザーに生体情報の提供を要求することにより（ユーザーに認識させて）生体情報を取得する方法について説明を行う。

【0070】図10および図11は本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【0071】図10において、図10(a)はスライドテーブル501が格納されている状態を示していて、図10(b)はスライドテーブルが引き出されている状態をそれぞれ示している。

【0072】本発明に係る記録再生装置（デッキ本体503）は、認証が必要になったときに、自動若しくは手動にて引き出されるスライドテーブル501を有し、スライドテーブル501上には生体情報検出電極301が設けられている。この生体情報検出電極301上に指の腹部を乗せることにより、ユーザー（操作者）の生体情報が読み取られ、この生体情報に基づいて個人認証が行われる。個人認証終了後、生体情報検出電極301は、自動若しくは手動にて、デッキ本体503内部に収納される。

【0073】ユーザー（装置使用者）認証は、図示しない記録媒体をデッキ本体503に挿入した場合や、ユーザーが所定の操作を行おうとして操作キー等を押下した場合などに、自動的に生体情報検出電極が現れる、個人認証の必要が明示的に示される。前述の通り、生体情報検出電極301上に指の腹部を乗せ、個人認証が行われ、認証が完了すると格納される。これにより、異物等の付着による生体情報検出電極301の汚染を防ぎ得る。

【0074】同様に、図11において、図11(a)はパネルドア602が格納されている状態を示していて、図11(b)はパネルドア602が開いている状態をそれぞれ示している。尚、図11は図10の他の例を示したものである。

【0075】本発明に係る記録再生装置（デッキ本体604）は、認証が必要になったときに、自動若しくは手動にて支点601をドア下部に持ち、手前に倒れるように開くパネルドア602の内側に引き出されるパネルドア602が設けられている。パネルドア602上には、生体情報検出電極301が配置されていて、この生体情報検出電極301上に指の腹部を乗せることにより、ユーザー（操作者）の生体情報が読み取られ、この生体情報に基づいて個人認証が行われ、個人認証終了後、パネルドア602は、自動若しくは手動にて、デッキ本体604内部に収納される。

【0076】ユーザー（装置使用者）認証は、図示しない記録媒体をデッキ本体604に挿入した場合や、ユーザーが所定の操作を行おうとして操作キー等を押下した場合などに、自動的に生体情報検出電極301が現れ、個人認証の必要が明示的に示される。前述の通り、生体情報検出電極301上に指の腹部を乗せ、個人認証が行われ、認証が完了すると格納される。これにより、異物等の付着による生体情報検出電極301の汚染を図10に示した場合と同様に防ぎ得る。

【0077】以上、生体情報検出手段である指認証装置により検出された生体情報と、記録再生装置に設けられ

た記憶手段または記録再生装置で使用する記録媒体に登録された指照合個人認証データとにより個人認証を行い、その結果に基づいて、当該記録再生装置で使用する記録媒体への記録や再生の制限を行う、本発明である生体情報による個人認証装置を具備した記録再生装置について説明したが、次に、これら本発明による複数の記録再生装置間における記録データの複写（ダビング）制御（制限）について説明を行う。

【0078】ここでは、上記個人認証情報および各個人毎の装置に対する設定条件が登録されている記録媒体、即ち、指照合個人認証データおよびそれらに対応した権利付与内容が登録されている記録媒体を第1の記録再生装置（再生側装置）により再生し、第2の記録再生装置（記録側装置）にて記録（ダビング）する場合について、図12および図13を参照しながら説明する。

【0079】図12は再生側装置および記録側装置の構成を示すブロック図であり、図13はダビング動作を示したフローチャートである。

【0080】図12において、再生側装置702aは、例えば、DVC（民生用デジタルVTR）等の個人認証データおよび各個人毎の装置に対する設定条件データが登録された記録媒体701aと、個人認証データおよび各個人毎の装置の設定条件データ読み取り手段704aと、個人認証データ一致比較手段705aと、ダビング許可禁止判定手段706aと、記録再生制御手段703aと、ケーブル708を介して記録側装置702bとデータのやりとりを行うデジタルインターフェース手段707aと、により構成される。

【0081】個人認証データおよび各個人毎の装置の設定条件データ読み取り手段704aは、記録媒体701aより個人認証データおよび各個人毎の装置に対する設定条件データを読み取る。個人認証データ一致比較手段705aは、ケーブル708よりデジタルインターフェース手段707aを介して記録側装置702bより供給される個人認証データおよび各個人毎の装置に対する設定条件データと、前記読み取り手段704aからの個人認証データおよび各個人毎の装置に対する設定条件データと、を比較する。ダビング許可禁止判定手段706aは、個人認証データ一致比較手段705aの比較結果に基づいてダビングの許可または禁止を判定してその結果を出力する。記録再生制御手段703aは、ダビング許可禁止判定手段706aの判定結果に基づいて前記記録媒体701aに対する再生の制御を行う。

【0082】同様に、記録側装置702bは、例えば、DVC（民生用デジタルVTR）等の個人認証データおよび各個人毎の装置に対する設定条件データが登録された記録媒体701bと、個人認証データおよび各個人毎の装置の設定条件データ読み取り手段704bと、個人認証データ一致比較手段705bと、ダビング許可禁止判定手段706bと、記録再生制御手段703bと、

ケーブル708を介して再生側装置702aとデータのやりとりを行うデジタルインターフェース手段707bと、により構成される。

【0083】個人認証データおよび各個人毎の装置の設定条件データ読み取り手段704bは、記録媒体701bより個人認証データおよび各個人毎の装置に対する設定条件データを読み取る。個人認証データ一致比較手段705bは、ケーブル708よりデジタルインターフェース手段707bを介して再生側装置702aより供給される個人認証データおよび各個人毎の装置に対する設定条件データと、前記読み取り手段704bからの個人認証データおよび各個人毎の装置に対する設定条件データと、を比較する。ダビング許可禁止判定手段706bは、個人認証データ一致比較手段705bの比較結果に基づいてダビングの許可または禁止を判定してその結果を出力する。記録再生制御手段703bは、ダビング許可禁止判定手段706bの判定結果に基づいて前記記録媒体701bに対する記録の制御を行う。

【0084】以上の構成において、記録再生装置間は、例えばIEEE1394などのインターフェース（ケーブル708、デジタルインターフェース手段707a、707b）を介してダビング可能な状態であるとする。ユーザーがダビングをしたい場合、例えば、再生側で再生キーを押下すると共に記録側でRECキーを押下するか、外部コントローラからダビングコマンドを出力（送信）する。何れの場合でも、IEEE1394等を介し、相手装置の（再生側装置は記録側装置の、記録側装置は再生側装置の）動作コマンドを知ることができ、ユーザーからダビング要求があったことを知ることができる（ステップT1）。

【0085】記録側再生側それぞれの装置においてダビング要求が確認されると、再生側装置702a並びに記録側装置702bは、それぞれ個人認証データが記録されている記録媒体（例えば、メモリ付きカセット）から、個人認証データ、およびその個人の装置の設定条件データを読みとる（ステップT2、T3）。そして、再生側装置702aは記録側装置702bで読みとった上記個人認証データ（およびその設定条件データ）をIEEE1394等のデジタルインターフェースを介して再生側装置702aへ伝送する。尚、逆に再生側装置702aで読みとったデータを記録側装置702bに伝送してもよい（ステップT4）。

【0086】さらに、再生側装置702aは、前記読みとった個人認証データ（およびその設定条件データ）と、伝送された記録側装置702bの個人認証データとを、個人認証データ一致比較手段705aで比較する。一致していなければ、記録テープと再生テープとは、それぞれ別の人の所有であると推定され、ダビング許可禁止判定手段706aによりダビング禁止の判定が為され、相手側装置（記録側装置）にダビング禁止信号をデ



ィジタルインターフェース手段707a, IEEE1394ケーブル708, およびィジタルインターフェース手段707bを介して伝送すると共にダビング動作を停止(禁止)する(ステップT5, T10, T11)。

【0087】前記個人認証データ一致比較手段705aでの比較結果が一致していた場合には、再生側装置702aで認証された個人の装置設定条件に「PLAY」はあるか、即ち、再生する権利を有するか(ステップT6)、また、記録側装置702bで認証された個人の装置設定条件に「REC」はあるか、即ち、記録する権利を有するか(ステップT7)が判定され、何れか一方でも満たさない(権利を有しない)場合には、ダビング動作を停止(禁止)する(ステップT10, T11)。

【0088】前記ステップT6, T7が共に条件を満たす場合には、ダビング許可禁止判定手段706aにより、ダビング許可の判定が為され、相手側装置(記録側装置)にダビング許可信号が、ィジタルインターフェース手段707a, IEEE1394ケーブル708, およびィジタルインターフェース手段707bを介して伝送されると共に、記録再生制御手段703a, 703bによりダビング動作が開始される(ステップT8, T9)。

【0089】なお、上記ステップT5, T6, T7の判定処理は、再生側装置702aの個人認証データ一致比較手段705aおよびダビング許可禁止判定手段706aによって行われるとして説明したが、記録側装置702bの個人認証データ一致比較手段705bおよびダビング許可禁止判定手段706bにて行うようにしても良い。

【0090】また、上記ダビング動作時には、記録媒体のデータのみコピーして、個人認証データや装置の設定条件等の記録は、原則コピーしないようにすることが望ましい。よって、本発明による個人認証データや装置の設定条件のデータを記録する記録媒体のデータをダビングする際、個人認証データや装置の設定条件を記録するデータは、全ての条件で、ダビングを禁止とする。

【0091】さらに、以上の個人認証データおよび装置の設定条件のデータを用いたダビング許可禁止動作は、前述のVTRのメモリ付きカセットに記憶した場合だけでなく、DVD-RAM DISCのTOC部分など、他の記録再生装置の記録媒体の特定箇所の場合でも全て当てはまる。

【0092】ところで、著作権侵害や不正コピー防止機能として、記録データを暗号化したりスクランブルをかけて記録するシステムが考案されていることは周知である。そこで、本発明の生体情報(個人認証データ)を、記録データを前記暗号化したりスクランブルをかけたリ、あるいは暗号やスクランブルを解くためのキーとして使用することが考えられる。この方法を用いることにより、データの秘匿性効果を格段に高めることが可能と

なる。以下、これについて説明を行う。

【0093】本発明の記録再生装置、または記録媒体に、生体情報(個人認証データ)の登録の為されたユーザーの個人認証データ、或いは認証データに所定の演算を施したものをを用いて(初期値として)、暗号やスクランブルのキーデータを発生させる。そして、このキーデータを用いてデータを暗号化、またはスクランブル化して、前記記録データを前記記録媒体に記録するようにする。尚、このキーデータ自体を記録媒体に記憶させておくことで、繰り返し再生を行うときなど、再生の度に、毎回、暗号やスクランブルのキーデータを発生(生成)する処理を省くことができる。

【0094】次に、既述の如く本発明の記録再生装置から個人認証データを入力し(個人認証を行い)、登録してある個人認証データと比較し、比較結果が一致していた場合にのみ再生動作が行われる。再生動作は、例えば、前記記録媒体から記録時に記録されていたキーデータを読み出し、読み出したキーデータに基づいて、同じく前記記録媒体から読み出された暗号化(符号化)またはスクランブル化された記録データに復号またはデスクランブル処理が施され、これにより復元された記録データが得られる。

【0095】以上により、秘匿性が非常に高い記録再生装置を実現することができる。尚、暗号化(符号化)またはスクランブル化された記録データを前記記録媒体に記録する際、暗号化(符号化)またはスクランブル化のためのキーデータを前記記録媒体に記憶させておかなくても、再生時に、個人認証データからキーデータを発生し、このキーデータに基づいて、記録媒体から読み出された暗号化(符号化)またはスクランブル化された記録データに復号またはデスクランブル処理を施すことにより、復元された記録データが得られ、同様に、秘匿性の非常に高い記録再生装置を実現することができるというまでもない。

【0096】次に、生体情報検出電極をリモコン装置に設けた本発明の生体情報を使用する記録再生装置について説明を行う。図14は本発明の実施の形態に係る生体情報検出電極を具備したリモコン装置を示すブロック図である。

【0097】図14(a)はリモコン装置の形態の一例を示したもので、リモコン801の表側には機能選択スイッチ803が複数配置されており、裏側には指を押つけて電気抵抗を検出する生体情報検出電極301が設置されている。

【0098】図14(b)は生体情報検出電極をリモコン装置に設けたVTR装置の構成を示したものである。リモコン801は、指を押つけて電気抵抗を検出する前記生体情報検出電極301と、前記電気抵抗を指全体の1次元パターンに変換するパターン入力部806と、機能選択スイッチ803で選択された機能に対応する機

能選択信号を出力する機能選択部804と、パターン入力部806の出力と機能選択部804の出力とから、例えば図14(c)に示す如くの少なくとも指の1次元パターンのコード、並びに機能選択コードの2つの情報を伝達するための領域を有するデータフォーマットから成る、リモコンコード信号を出力するリモコンコード生成部805と、リモコンコード信号を赤外線などの送信信号に変換して出力する送信部807とから構成される。

【0099】また、VTR812は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部808と、リモコンコード信号をデコードするリモコンコードデコード部809と、個人認証を行う個人認証処理部810と、VTR装置の記録、再生等の動作の許可または禁止処理を行う制御部811とから構成される。

【0100】次に、以上のように構成された生体情報検出電極をリモコン装置に設けたVTR装置の動作について説明を行う。

【0101】先ず、リモコン801の表側の機能選択スイッチ803が押下されると、機能選択部804で、前記各スイッチの機能に対応した機能選択信号を発生し、リモコンコード生成部805に出力する。一方、パターン入力部806では、リモコン裏側の生体情報検出電極301に指が押しつけられると、生体情報検出電極301で検出された電気抵抗値を、指全体の1次元パターン（以下、単に指の1次元パターンという）に変換し、前記リモコンコード生成部805に出力する。

【0102】リモコンコード生成部805では、パターン入力部806より指の1次元パターンが入力されている場合には、この指の1次元パターンと、機能選択部804から入力された機能選択信号とを、例えば図14(c)に示す如くのデータフォーマットにて、リモコンコード信号に変換し、送信部807に出力する。一方、パターン入力部806より指の1次元パターンが入力されていない場合には、リモコンコード信号の出力を行わない。

【0103】送信部807では、パターン入力部806よりリモコンコード生成部805に指の1次元パターンが入力されている場合に限り、リモコンコード生成部805から入力されたリモコンコード信号を、赤外線などの送信信号に変換して出力する。

【0104】VTR812では、受信部808にて、前記リモコン801からの送信信号を受信する。受信部808で受信された信号は、例えば図14(c)に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部809に出力される。リモコンコードデコード部809では、受信部808より入力されたリモコンコード信号をデコードし、指の1次元パターンを個人認証処理部810へ出力すると共に、機能選択信号を制御部811に出力する。

【0105】個人認証処理部810では、リモコンコードデコード部809より入力された指の1次元パターンと、図示しない個人認証情報用メモリ102に登録された個人認証情報（指情報）、または図示しない記録媒体であるカセットテープのMICやDVD-RAMのTOC等に登録された個人認証情報（および各個人毎の装置に対する設定条件データ）とから、個人認証処理を行い、その結果を制御部811へ出力する。

【0106】制御部811では、個人認証処理部810より供給された個人認証処理結果とリモコンコードデコード部809より供給された機能選択信号に従って、図2および図3で説明した如くに、即ち、前記個人認証処理部810より個人認証がパスしない場合には、記録、再生等のVTR812に対する一切の操作が禁止されて、個人認証をパスした場合には、前記図示しない記録媒体に登録された各個人毎の装置に対する設定条件データの内の、個人認証された者の装置に対する設定条件データの登録内容（認証された者が有する記録や再生等を行う権利）に基づいて、VTR812に対する記録、再生等の動作が為される。

【0107】なお、前記記録媒体への新たな登録は、勿論、このリモコン装置を用いて行っても良いし、VTR装置で行っても良い。

【0108】さて、上述のリモコン装置は、前記指全体の1次元パターンと機能選択信号共に揃ったとき、即ち、リモコンコード生成部805で、図14(c)に示す如くのデータフォーマットにて、リモコンコード信号が生成（変換）されることにより、送信部807を介してVTR812に出力される。リモコンコード信号の生成は、例えば、図15(a)および図15(b)に示す2通りの手順により、リモコンコード生成部805にて行われる。以下、リモコンコード信号の生成手順について図15を参照しながら説明を行う。図15はリモコンコード信号の生成手順の2つの例を示すフローチャートである。尚、以下の手順では、認証処理は無条件でパスするものとする。

【0109】リモコンコード信号の生成例、即ち、図15(a)に示す例の場合、リモコンコード生成部805では、以下の手順にて機能選択信号と指全体の1次元パターンの入力を受け付け、リモコンコードを生成出力する。

【0110】先ず、リモコンコード生成部805は、リモコン801の機能選択スイッチ803が押下されることにより、機能選択信号が入力されると、生体情報検出電極301に指が押しつけられることにより検出された電気抵抗値に基づいて、パターン入力部806により変換出力される、指全体の1次元パターンの入力待ち状態となる（ステップU1、U2、U3）。

【0111】そして、生体情報検出電極301に指が押しつけられると、パターン入力部806は、生体情報検



出電極 301 により検出された電気抵抗値に基づいて指全体の 1 次元パターンをリモコンコード生成部 805 に出力する (ステップ U4, U5)。

【0112】これにより、リモコンコード生成部 805 は、例えば、前記図 14 (c) に示す如くのデータフォーマットにてリモコンコード信号を生成 (変換) ・出力し (ステップ U6)、送信部 807 を介し、赤外線などの送信信号として、例えば VTR 812 に送信する。

【0113】次に、リモコンコード信号の他の生成例、即ち、図 15 (b) について説明を行う。図 15 (b) に示す例の場合、リモコンコード生成部 805 では、以下の手順にて機能選択信号と指全体の 1 次元パターンの入力を受け付け、リモコンコードを生成出力する。

【0114】まず、リモコンコード生成部 805 は、リモコン 801 の生体情報検出電極 301 より指全体の 1 次元パターンの入力があると、機能選択スイッチ 803 の押下待ち状態、即ち、機能選択部 804 が発生する機能選択信号の入力待ち状態となる (ステップ V1, V2, V3)。

【0115】そして、リモコン 801 の機能選択スイッチ 803 が押下されることにより、機能選択信号が入力されると、リモコンコード生成部 805 は、前記生体情報検出電極 301 より、継続して指全体の 1 次元パターンの入力があるか否か (指全体の 1 次元パターン入力が完了したか否か) の判別を行う。

【0116】リモコンコード生成部 805 は、継続して指全体の 1 次元パターンの入力がある場合には、例えば、前記図 14 (c) に示す如くのデータフォーマットにてリモコンコード信号を生成 (変換) ・出力し (ステップ V6)、送信部 807 を介し、赤外線などの送信信号として、例えば VTR 812 に送信する。一方、継続して指全体の 1 次元パターンの入力がない (機能選択信号が入力されたタイミングに指全体の 1 次元パターンの入力がない) 場合には、ステップ V1 にもどり、リモコン 801 の生体情報検出電極 301 より指全体の 1 次元パターンの入力待ち状態となる。

【0117】ところで、上記図 15 (a) と図 15 (b) に示すそれぞれの場合の違いとして、例えば、図 15 (b) の場合には、機能選択信号と指全体の 1 次元パターンの入力が、リモコンコード生成部 805 に対してほぼ同時に行われる必要があるのに対し、図 15 (a) の場合には、必ずしも同時である必要はない点が挙げられる。尚、送信信号出力後の VTR 812 の動作は、前記図 14 で説明した VTR 812 の動作説明と同様であるので省略する。

【0118】次に、同時に複数の装置の操作が可能な、いわゆるマルチリモコン装置であって、上記図 14 および図 15 で説明した機能を有するリモコン装置について説明を行う。

【0119】図 16 は本発明の実施の形態に係る生体情

報検出電極を具備したマルチリモコン装置および被制御装置を示すブロック図である。

【0120】図 16 (a) は生体情報検出電極を備えたマルチリモコン装置と被制御装置として、例えばテレビジョン受像機と VTR 装置との構成を示したものである。リモコン 801 は、指を押しつけることにより電気抵抗を検出する生体情報検出電極 301 と、前記電気抵抗を指全体の 1 次元パターンに変換するパターン入力部 806 と、機能選択スイッチ 803 で選択された機能に対応する機能選択信号を出力する機能選択部 804 と、パターン入力部 806 の出力と機能選択部 804 の出力とから、例えば図 16 (c) に示す如くの少なくとも、装置選択コード、指の 1 次元パターンのコード、並びに機能選択コードの 3 つの情報を伝達するための領域を有するデータフォーマットから成るリモコンコード信号を出力するリモコンコード生成部 805 と、リモコンコード信号を赤外線などの送信信号に変換して出力する送信部 807 とから構成される。

【0121】また、テレビ 813 は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部 808 と、リモコンコード信号をデコードするリモコンコードデコード部 815 と、前記リモコンコード信号より生成 (デコード) された装置選択信号および機能選択信号に基づいてテレビジョン受像機の各種動作を制御する制御部 816 とから構成される。

【0122】さらに、VTR 814 は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部 808 と、リモコンコード信号をデコードするリモコンコードデコード部 817 と、個人認証を行う個人認証処理部 818 と、前記リモコンコード信号より生成 (デコード) された装置選択信号および機能選択信号と前記個人認証処理部 818 からの出力信号に基づいて、VTR 装置の記録、再生等の動作の許可または禁止処理を行う制御部 811 とから構成される。

【0123】図 16 (b) はリモコン装置の形態の一例を示したもので、リモコン 801 の表側には、例えば、TV 用と VTR 用の機能選択スイッチ 803 が複数配置されており、裏側には指を押しつけて電気抵抗を検出する図示しない生体情報検出電極 301 が設置されている。

【0124】次に、以上のように構成された生体情報検出電極を具備したマルチリモコン装置および被制御装置であるテレビジョン受像機および VTR 装置の動作について説明を行う。

【0125】まず、リモコン 801 の表側の機能選択スイッチ 803 が押下されると、機能選択部 804 で、前記各スイッチの機能に対応した機能選択信号を発生し、リモコンコード生成部 805 に出力する。一方、パターン入力部 806 では、リモコン裏側の生体情報検出電極 301 に指が押しつけられると、生体情報検出電極 301

1で検出された電気抵抗値を、指の1次元パターン（指全体の1次元パターン）に変換し、前記リモコンコード生成部805に出力する。

【0126】リモコンコード生成部805では、パターン入力部806より指の1次元パターンが入力されている場合には、この指の1次元パターンと、機能選択部804から入力された装置選択信号と機能選択信号とを、例えば図16(c)に示す如くのデータフォーマットにて、リモコンコード信号に変換し、送信部807に出力する。尚、パターン入力部806より指の1次元パターンが入力されていない場合には、リモコンコード信号の出力は行われない。

【0127】送信部807では、リモコンコード生成部805から入力されたリモコンコード信号を、赤外線などの送信信号に変換して出力する。

【0128】一方、VTR814およびテレビ813などの装置では、リモコン801より出力された送信信号を受信部808で受信する。受信部808では、受信した信号を例えば図16(c)に示す如くのデータフォーマットのリモコンコード信号に変換する。

【0129】これ以後の処理は、個人認証を行う装置と個人認証を行わない装置（本実施の形態ではVTR814とテレビ813）で処理内容が異なる。

【0130】即ち、個人認証を行う装置であるVTR814では、受信部808にて、前記リモコン801からの送信信号を受信する。受信部808で受信された信号は、例えば図16(c)に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部817に出力される。リモコンコードデコード部817では、受信部808より入力されたリモコンコード信号をデコードし、指の1次元パターンを個人認証処理部818へ出力すると共に、装置選択信号および機能選択信号を制御部819に出力する。

【0131】個人認証処理部818では、リモコンコードデコード部817より入力された指の1次元パターンと、図示しない個人認証情報メモリに登録された個人認証情報（指情報）、または図示しない記録媒体であるカセットテープのMICやDVD-RAMのTOC等に登録された個人認証情報（および各個人毎の装置に対する設定条件データ）とから、個人認証処理を行い、その結果を制御部819へ出力する。

【0132】制御部819では、リモコンコードデコード部817から入力された装置選択信号の値が、装置選択信号の値がVTRを示している場合には、リモコンコードデコード部817から入力された機能選択信号と、個人認証処理部818より供給された個人認証処理結果にしたがい、前記図2および図3で説明した如く、即ち、前記個人認証処理部818において個人認証がパスしない場合には、記録、再生等のVTR814に関する一切の操作が禁止され、個人認証をパスした場合には、

前記図示しない記録媒体に登録された各個人毎の装置に対する設定条件データの内の、個人認証された者の装置に対する設定条件データの登録内容（認証された者が有する記録や再生等を行う権利）に基づいて、VTR814に対する記録、再生等の制御が為される。

【0133】一方、制御部819は、リモコンコードデコード部817から入力された装置選択信号の値が、VTRを示していない場合には、リモコンコードデコード部817から入力される機能選択信号は無視され、VTR814に関する記録、再生等の一切の制御が禁止される（為されない）。

【0134】次に、個人認証を行わない装置であるテレビ813では、受信部808にて、前記リモコン801からの送信信号を受信する。受信部808で受信された信号は、例えば図16(c)に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部815に出力される。リモコンコードデコード部815では、受信部808より入力されたリモコンコード信号をデコードし、装置選択信号および機能選択信号を制御部816に出力する。

【0135】制御部816では、リモコンコードデコード部815から入力された装置選択信号の値が、テレビを示している場合には、リモコンコードデコード部815からの機能選択信号を受け付け、これに基づいてテレビジョン受像機の各種動作の制御が為される。

【0136】一方、リモコンコードデコード部815から入力された装置選択信号の値が、テレビを示していない場合には、リモコンコードデコード部815から入力された機能選択信号は無視され、これにより、テレビ813に関する一切の制御が禁止される（為されない）。

【0137】

【発明の効果】以上述べたように本発明によれば、記録再生装置に個人認証手段を装備し、装置を動作させる際、個人認証動作を行うようにしたので、装置が盗難にあった場合、正常に動作しないため盗難防止になる。また、個人使用（パーソナルユース）のための装置の場合、第三者による記録が出来ないため誤記録、誤消去を防ぐことができると共に、テープなどの媒体に記録されているパーソナル情報を保護することができる。さらに、認証手段の認証状況を、LED、ブザー、あるいはモニタ表示することにより、認証動作の進捗状況等を容易に確認することができる。

【0138】また、記録媒体自体に個人認証データを記録しておき、このデータをもとに個人認証を行い、カセットテープの管理を行うようにする構成としたので、誤って他人の重要な情報を消去してしまったり、或いは他人に消されることがなく、他人に見せたくないデータを保護することができ、盗難にあってもデータを再生される心配がない、などの効果が得られる。

【0139】そして、個人認証手段と記録再生装置の動

作スイッチとを兼ねた構成としたことにより、ユーザーは個人認証が行われていること意識することなく本発明の記録再生装置を使用することができる。

【0140】さらに、認証に際し（必要に応じ）、自動的に生体情報検出電極が現れるようにしたので、個人認証の必要が明示的に示されると共に、使用後、格納されるようにしたことにより、生体情報検出電極への異物等の付着を防止でき、生体情報検出電極の汚染を防ぐことができる。

【0141】また、再生テープから記録テープへとダビングする際、個人認証動作を行い、その結果に基づいてダビングの制限を設けるようにしたので、ソース側テープの著作権やプライバシーなどを、保護することができる。

【0142】さらに、暗号化またはスクランブルされた記録データを、DVCやDVD-RAM等の記録媒体へ記録する際に、暗号化またはスクランブルを解くキーデータとして、登録されたユーザーの個人認証データそのまま、或いは認証データに所定の演算を施したものを用い、暗号化やスクランブルのためのキーデータを発生させ、このキーデータを用いて前記記録データを暗号化またはスクランブルし、記録するようにしたので、秘匿性の非常に高い記録再生装置を実現することが可能となる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態に係る生体情報による個人認証装置を具備した記録再生装置を示すブロック図である。

【図2】個人認証動作手順を示したフローチャートである。

【図3】メモリインカセットのメモリのデータストラクチャ例である。

【図4】本発明で個人認証を行うための生体情報検出手段として使用される指認証装置の一例を示すブロック図である。

【図5】指紋入力部を構成する表面形状センサの具体的な構成を示す図である。

【図6】指表面の抵抗値の測定原理を説明するための指紋入力部の等価回路である。

【図7】指認証装置の生体情報検出電極より得られる指

紋情報を示す図である。

【図8】指がスイッチキーを押している状態を示した図である。

【図9】指がスイッチキーを引いている状態を示した図である。

【図10】本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【図11】本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【図12】再生側装置および記録側装置の構成を示すブロック図である。

【図13】ダビング動作を示したフローチャートである。

【図14】本発明の実施の形態に係る生体情報検出電極を具備したリモコン装置を示すブロック図である。

【図15】リモコンコード信号の生成手順の2つの例を示すフローチャートである。

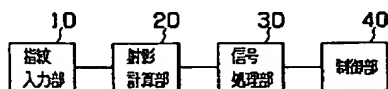
【図16】本発明の実施の形態に係る生体情報検出電極を具備したマルチリモコン装置および被制御装置を示すブロック図である。

【図17】従来の記録再生装置の構成を示すブロック図である。

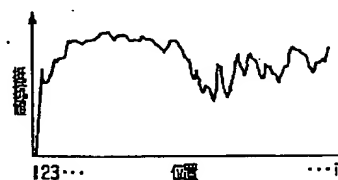
#### 【符号の説明】

- 101…指認証装置（検出部）
- 102…個人認証情報用メモリ
- 103…CPU
- 104…ROM
- 105…RAM
- 106…D/A変換器
- 107…EJECT用モータ
- 108…D/A変換器
- 109…ローディング・モータ
- 110…D/A変換器
- 111…サプライ・リールモータ
- 112…D/A変換器
- 113…テイクアップ・リールモータ
- 114…LED
- 115…LED
- 116…プザー

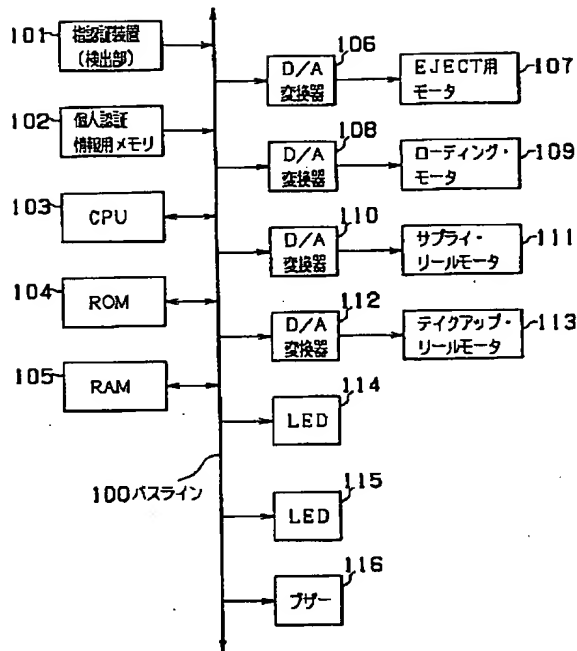
【図4】



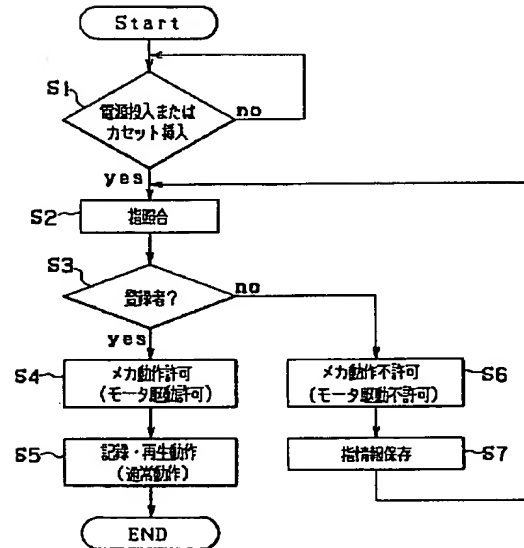
【図7】



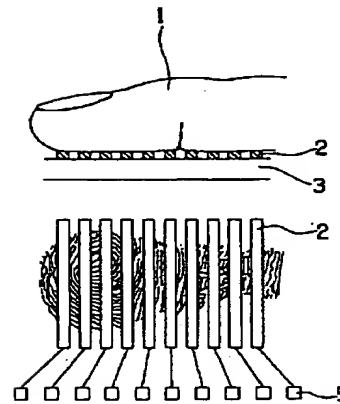
【図1】



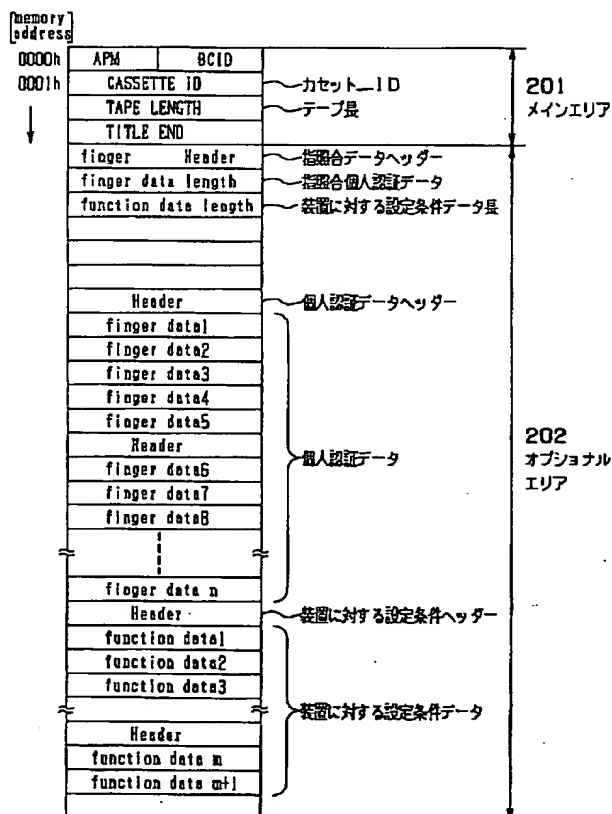
【図2】



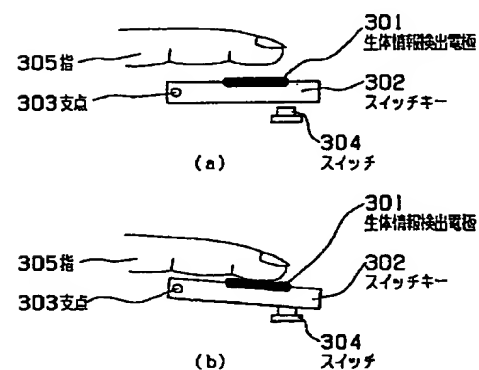
【図5】



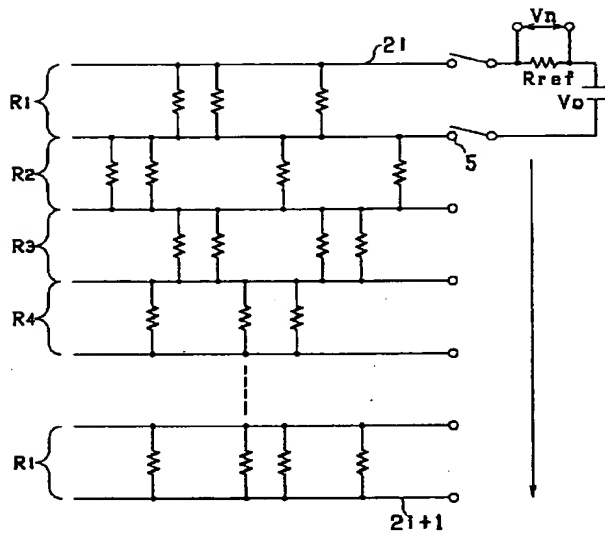
【図3】



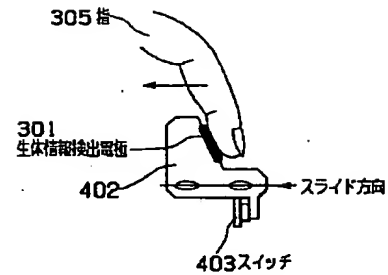
【図8】



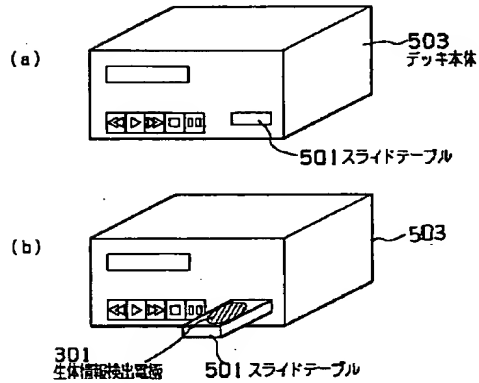
【図6】



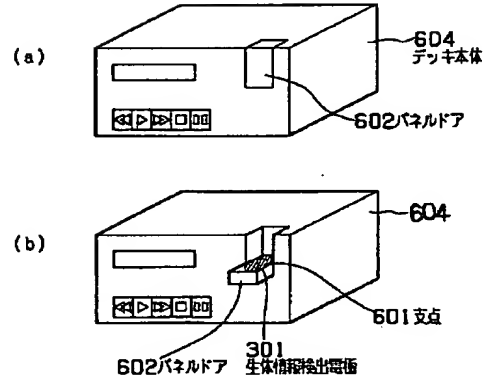
【図9】



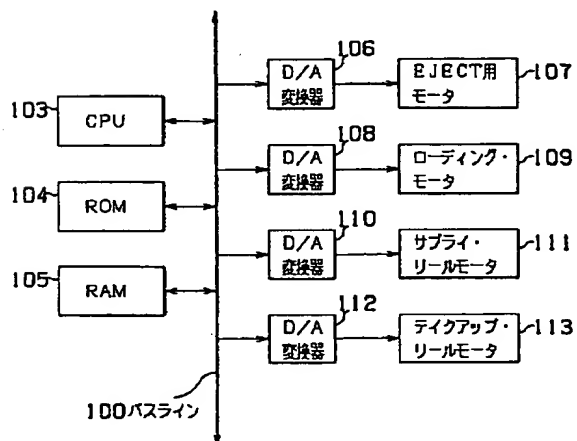
【図10】



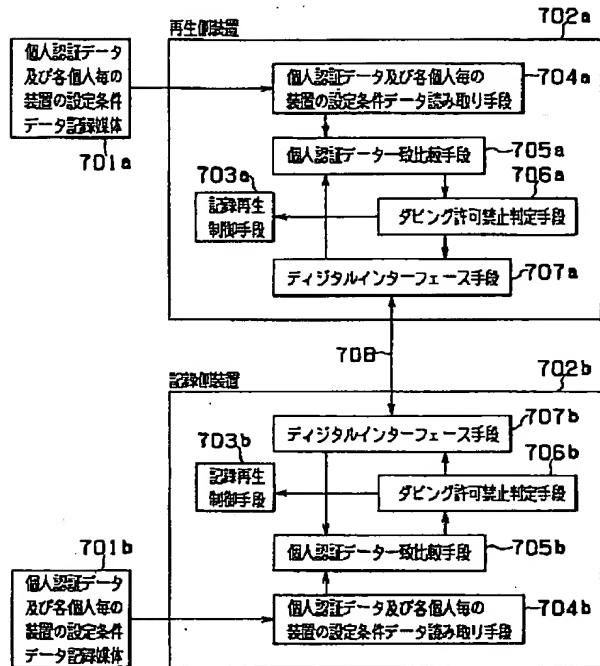
【図11】



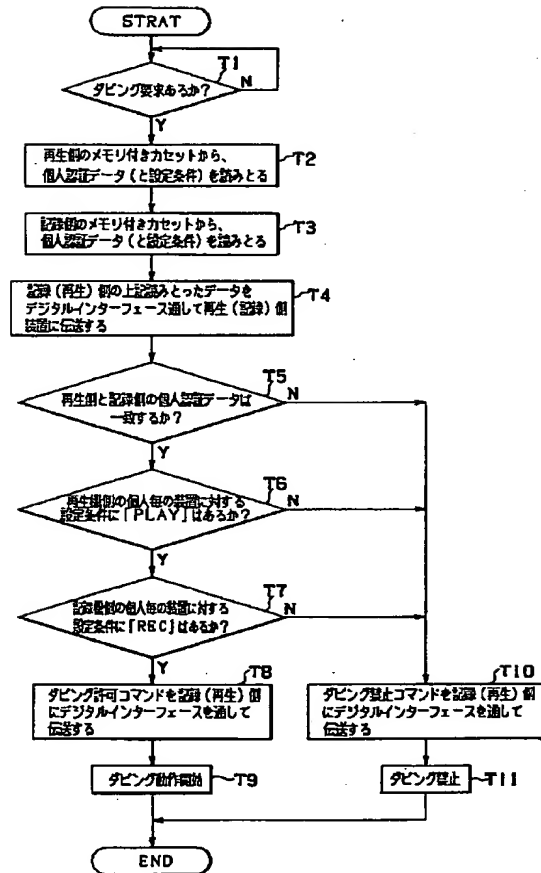
【図17】



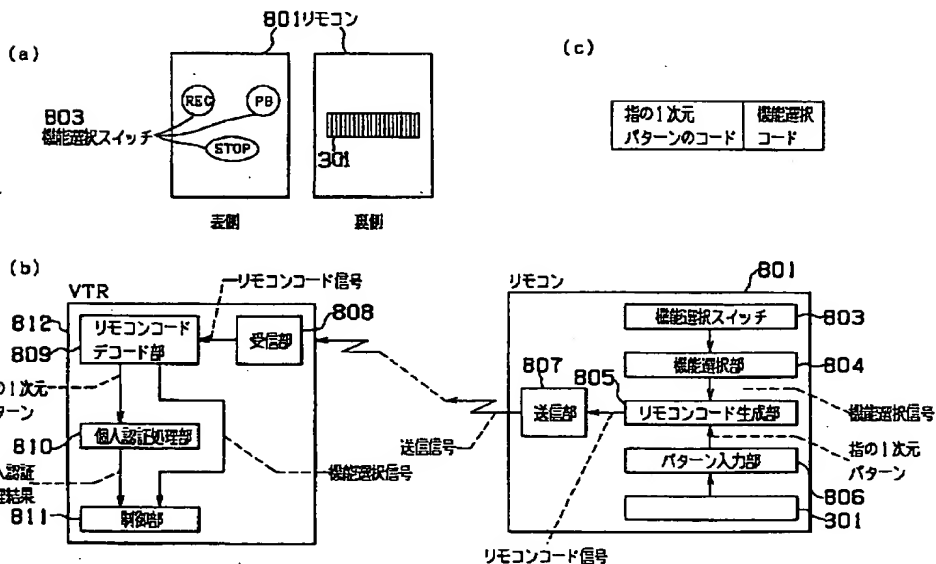
【図 12】



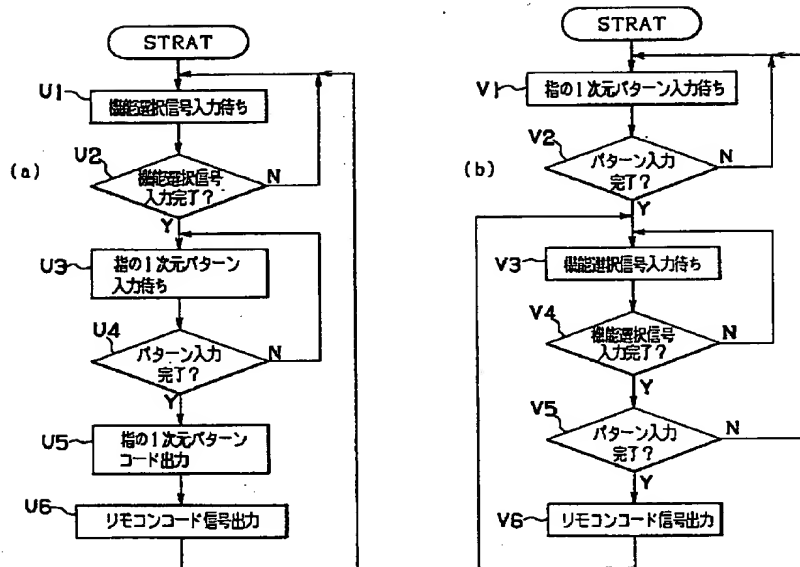
【図 13】



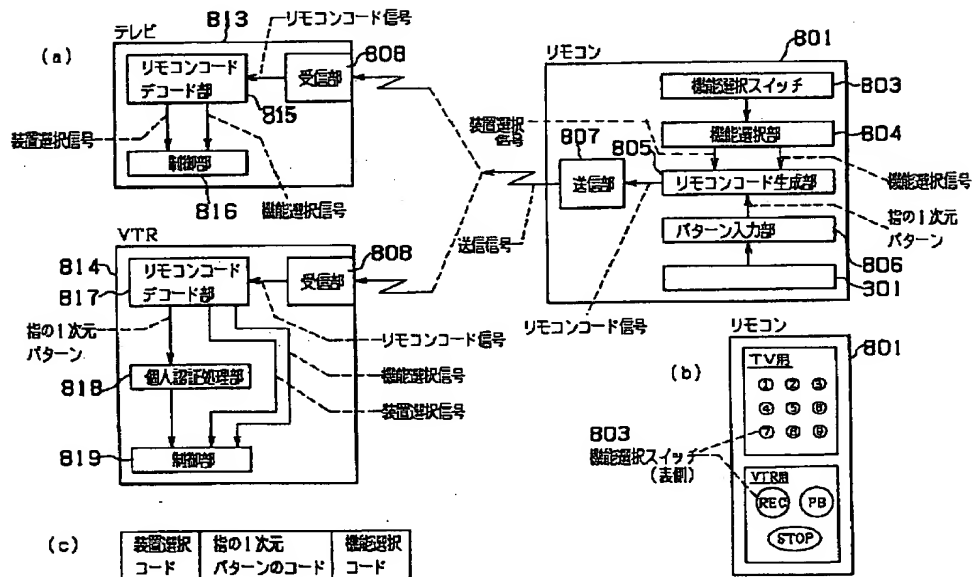
【図 14】



【図15】



【図16】



フロントページの続き

(72) 発明者 奥山 武彦  
 神奈川県横浜市磯子区新杉田町8番地 株  
 式会社東芝マルチメディア技術研究所内  
 (72) 発明者 山田寺 真司  
 神奈川県横浜市磯子区新杉田町8番地 株  
 式会社東芝マルチメディア技術研究所内

(72) 発明者 福島 道弘  
 神奈川県横浜市磯子区新杉田町8番地 株  
 式会社東芝マルチメディア技術研究所内  
 (72) 発明者 大沢 真一  
 東京都港区新橋3丁目3番9号 東芝エ  
 ー・ビー・イー株式会社内

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**